OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Commissariat à la protection de la vie privée du Canada | Office of the Privacy Commissioner of Canada

Statement

November 26, 2019

Remarks by the Information and Privacy Commissioner for British Columbia regarding the joint AggregateIQ investigation.

Vancouver, British Columbia

The Information and Privacy Commissioner for British Columbia made the following statement during a joint press conference at Simon Fraser University in Vancouver.

(Check against delivery)

Good morning. My name is Michael McEvoy. I am the Information and Privacy Commissioner for British Columbia. With me is Daniel Therrien, Privacy Commissioner of Canada.

We are here this morning to report to you the results of our joint investigation into how AggregateIQ, a company based in Victoria, BC Canada, collected and used the personal information of voters in a number of jurisdictions, and whether it took the appropriate and necessary steps to protect the personal information of those voters.

Let me begin by saying that when it comes to collecting and using people's personal information, companies that operate on a global and national scale cannot simply pick and choose the rules they wish to follow. This applies to Canadian companies that operate across jurisdictions.

AggregateIQ is one such company.

AIQ, as they are commonly known, is a small firm that operates on a large scale. They offer a variety of data-related services to political parties and campaigns, including microtargeted political ads.

The company gained initial media prominence because of their work for leave forces in the European Union referendum and connections with SCL Elections and their subsidiary company Cambridge Analytica.

Stories that this Canadian company may have improperly used voter information during the referendum caused my office and Commissioner Therrien's to join forces to investigate whether its foreign actions violated BC and federal law.

Subsequently, the investigation was expanded to encompass AIQ's US activities. They were provided with voter information for millions of Americans, including psychographic profiles that were based, at least in part, on the Facebook data harvested for Cambridge Analytica. Finally we examined AIQ's political campaign work in British Columbia and Canada.

Again I stress, though while some of these campaigns took place in foreign jurisdictions, where AIQ may have been subject to those laws, they and every other Canadian company doing work abroad, still remain subject to the privacy laws in this country.

These provincial and federal laws are based on consent, and our analysis and findings are focused on whether individuals provided consent for how their personal information was processed by AIQ.

Our investigation examined two main questions. First, did individuals consent to how AIQ used their personal information, as is required by our provincial and federal privacy laws? And second, did AIQ have adequate security measures in place to protect that personal information?

While we found that some of AIQ's services were covered by the consent of individuals, in many other instances, they were not. This includes microtargeted online profiling using social media which was clearly not based on consent.

Most concerning was AIQ's work in the US. In the report we describe how the company built a database to store and organize a vast amount of personal information about voters.

This information was provided by SCL Elections and Cambridge Analytica. It came from a variety of sources, including social media scraping and the data that Dr. Aleksandr Kogan obtained from Facebook and organized into psychographic profiles for the purpose of voter targeting.

We also examined AIQ's data security practices. We found that they left usernames, passwords, and encryption keys to some of its databases exposed, putting at risk the personal information of 35 million voters in the US, the UK, and BC.

In doing so, AIQ failed to take reasonable security measures to ensure that personal information under its control was secure from unauthorized access or disclosure.

Our report makes two recommendations. The first concerns data use and retention. In the future, AIQ must ensure that the data it uses is obtained with consent and that it deletes all personal information in its custody that is no longer necessary for legal or

business purposes. The company has agreed to do so. [In response to our demand, AIQ has provided a sworn affidavit to that effect.]

Second, AIQ must undertake a number of measures to better protect the personal information it holds. Again the company has agreed to this and has undertaken some work to date. We intend to follow up with AIQ in the coming months to confirm that they have implemented both of our recommendations in full.

This investigation's message is clear; that Canadian organizations operating globally must know the rules at home and abroad. They must ensure that they understand, and comply with, their legal responsibilities in Canada, even when they are also operating in other jurisdictions.

This what the global citizenry expects. This is what we, as regulators, expect.

My colleague, Commissioner Daniel Therrien, will now speak to some of the overarching issues surrounding this investigation, highlighting the need for law reform in this area and to ensure that the public is in fact properly protected.

For more information, please contact:

Office of the Information and Privacy Commissioner for British Columbia

Jane Zatylny A/Senior Communications Manager

jzatylny@oipc.bc.ca

250-415-3283